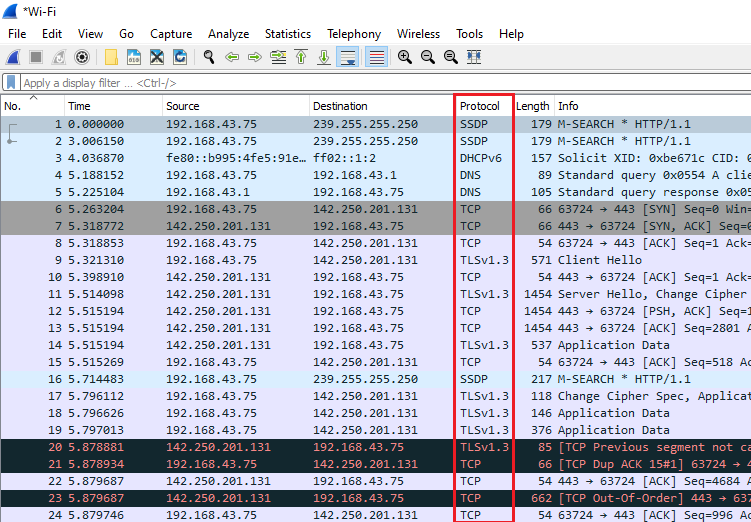
**گزارش دستورکار دوم آزمایشگاه درس شبکه­های کامپیوتری**

نگار موقتیان، 9831062

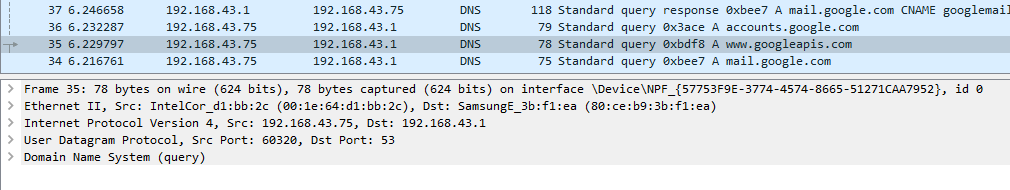
1. **پروتکل­های مشاهده شده در بسته­های شنود شده**

لیستی از پروتکل­های مشاهده شده شامل موارد زیر است:

TLSv1.3 – TLSv1.2 – TCP – SSLv2 – SSDP – QUIC – MDNS – HTTP – DNS – DHCPv6 – ARP

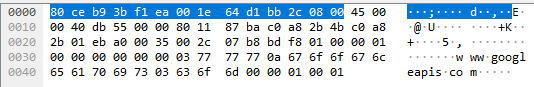


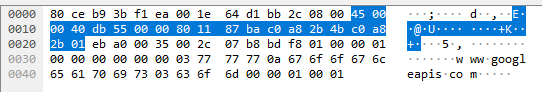
1. **پروتکل­های استفاده شده در لایه­های مختلف یک بسته**

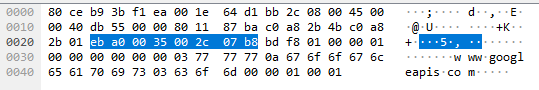
شکل زیر اطلاعات مربوط به بستۀ انتخاب شده را نشان می­دهد.

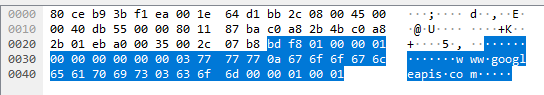
با توجه به این اطلاعات پروتکل­های استفاده شده در لایه­های مختلف مانند زیر است:

1. Physical Layer: wire – interface: Wi-Fi و Link Layer: Ethernet II
2. Network Layer: IPv4
3. Transport Layer: UDP
4. Application Layer: DNS

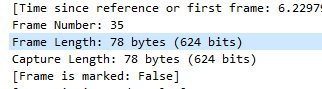
همچنین با توجه به داده­هایی که در پایین صفحه نشان داده می­شود می­توان گفت بیت­های داده به ترتیب لایه­ها قرار گرفته­اند. برای مثال در بستۀ فوق قرارگیری بیت­های مربوط به هر لایه به ترتیب زیر می­باشد (از لایه اول تا چهارم)



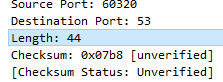




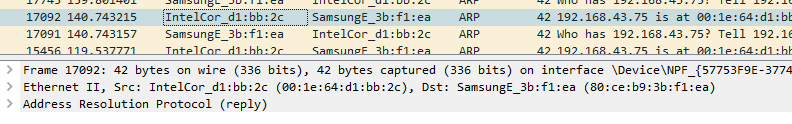
با توجه به اطلاعات این قسمت طول فریم این بسته 78 بایت است.



به علاوه طول بستۀ لایه Transport طبق اطلاعات زیر 44 بایت است.

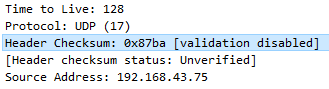


1. **بسته­هایی که بدون پروتکل­های لایه­های Network، Transport و Application هستند**

بله، مطابق شکل زیر بسته­هایی که از پروتکل ARP (که پروتکلی برای یافتن آدرس لایۀ پیوند و ارتباطش با آدرس لایۀ شبکه است) استفاده کرده­اند چنین ویژگی­ای دارند.

1. **مقدار Checksum در پروتکل IP**

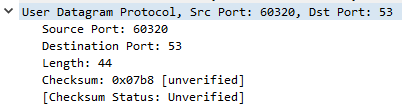
با توجه به این قسمت مقدار Checksum برابر است با34746 (87BA)16 =.



1. **شماره پورت و مقدار Checksum در پروتکل­های TCP و UDP**

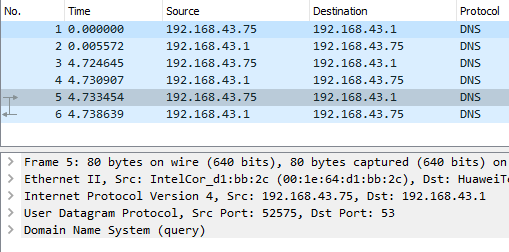
با توجه به این قسمت شماره پورت مبدا 60320 و شماره پورت مقصد 53 می­باشد. به طور کلی شماره پورت راهی برای مشخص کردن پردازه­ای است که زمانی که بسته به سرور می­رسد باید به آن تحویل داده شود. شمارۀ IP سیستم انتهایی را مشخص کرده و شماره پورت مشخص می­کند بسته مربوط به کدام پردازه (یا application) روی این سیستم است.

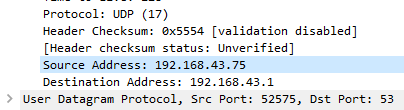
همچنین با توجه به شکل زیر مقدار Checksum برابر است با1976 (07B8)16 =.



1. **پروتکل لایۀ Transport، آدرس IP مقصد و اطلاعات مربوط سرآیند لایۀ دوم**

با توجه به شکل زیر می­توان گفت که این بسته برای انتقال در لایۀ Transport از پروتکل UDP استفاده می­کند. همچنین آدرس IP مقصد آن برابر است با 192.168.43.1.



همچنین با توجه به اطلاعات لایۀ دوم آدرس مبدا آن برابر با 192.168.43.75 و آدرس مقصد آن برابر با 192.168.43.1 می­باشد.

1. **آدرس مشترک میان قسمت قبل و خروجی دستور ipconfig**

با توجه به خروجی دستور ipconfig آدرس IP مربوط به سیستمی که از آن استفاده می­کنیم برابر است با 192.168.43.75 که همان آدرس مبدا در قسمت قبل آزمایش است. بنابراین می­توان گفت بستۀ فوق از طرف سیستم ما ارسال شده­ است.

1. **Type استفاده شده در پروتکل DNS در اجرای دستور Ping**

با توجه به اطلاعات زیر در این بخش از Type A استفاده شده­است.



پاسخ این query یک hostname و آدرس IP مربوط به آن را ذخیره می­کند. بنابراین می­توان گفت از این درخواست برای یافتن IP سرور گوگل با توجه به hostname آن استفاده شده­است.

1. **Type استفاده شده در پروتکل DNS در اجرای دستور nslookup**

با توجه به اطلاعات زیر در این بخش از Type PTR استفاده شده­است.

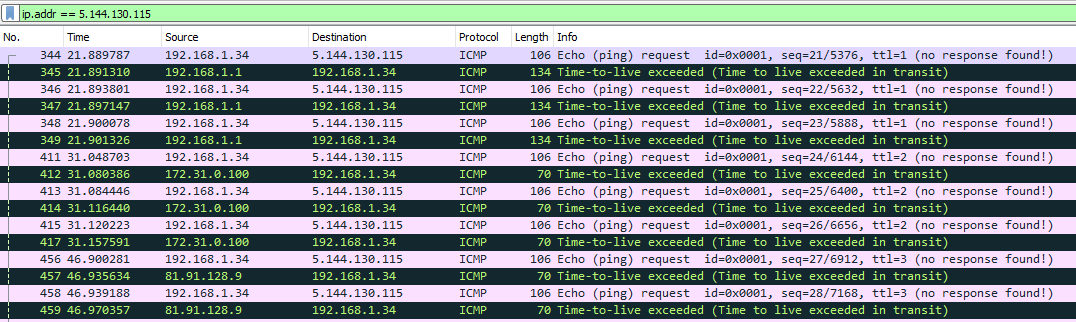


پاسخ این query برعکس کاری است که DNS در حالت عادی انجام می­دهد. بنابراین می­توان گفت از این درخواست برای یافتن hostname مربوط به IP ای با شمارۀ 1.1.1.1 استفاده شده­است.

1. **دیگر Type های استفاده شده در پروتکل DNS**

از دیگر type هایی که در پروتکل DNS استفاده می­شوند می­تواند به موارد زیر اشاره کرد:

1. NS: مشخص می­کند کدام سرور حاوی رکوردهای اصلی DNS مربوط به یک دامنه است و برای یافتن IP دامنۀ مورد نظر باید به کجا مراجعه کنیم.
2. CNAME: مشخص می­کند نام اصلی یک سرور چیست (گاهی برای سهولت در استفادۀ کاربران نام دیگری به جای نام اصلی سرور به طور متداول استفاده می­شود).
3. MX: سرور ایمیل SMTP مربوط به دامنه را مشخص می­کند.
4. **استفاده از Display Filter**

با توجه به فیلتر توصیف شده در دستورکار خروجی برنامه مطابق شکل زیر می­باشد.

همانطور که مشاهده می­شود این فیلتر تمام بسته­هایی را نشان می­دهد که آدرس IP مبدا و یا مقصد آن برابر با IP وبسایت p30download باشد. همچنین تمام پروتکل­های استفاده شده ICMP می­باشند زیرا دستوراتی مانند tracert و ping برای دریافت اطلاعات گره­ها از پیغام­های ICMP (Internet Control Message Protocol) استفاده می­کنند.

1. **بررسی مقادیر ICMP Type و IP Layer TTL**

با توجه به اطلاعات زیر در این بخش از Type 8 که مربوط به یک درخواست ping می­باشد استفاده شده­است.



همچنین مقدار TTL در پروتکل IP برابر است با 1.



1. **هدف از تغییر TTL در بسته­های ارسال شده توسط دستور tracert**

در صورتی که بسته­ها را به ترتیب بررسی کنیم متوجه می­شویم که مقدار TTL در هر چند بستۀ متوالی یکی افزایش می­یابد. هدف دستور tracert بررسی و شناسایی هر یک از گره­های موجود در مسیر تا گره مقصد است. همچنین می­دانیم TTL طول عمر بسته را مشخص می­کند. بنابراین با تغییر طول TTL می­توانیم آخرین گره­ای که بسته به آن می­رسد را مشخص کرده و اطلاعات آن گره را استخراج کنیم و از این طریق تمام گره­های موجود در طول مسیر به ازای TTL های مختلف را بررسی کنیم.

1. **استفاده از فیلتر ip.proto**

طبق جدول موجود در لینک زیر شمارۀ 6 معادل با پروتکل TCP می­باشد.

<https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers>

بنابراین این فیلتر بسته­هایی که از پروتکل TCP استفاده کرده­اند را نشان می­دهد. البته این فیلتر با فیلتر TCP متفاوت است و تنها بسته­هایی که پروتکل آن­ها TCP است را نشان نمی­دهد، بلکه بسته­هایی با پروتکل­های متفاوت (مانند ICMP و TLS) که از پروتکل TCP استفاده می­کنند را هم نمایش می­دهد.